Go ahead, we're listening.SM

Front End Security Architecture as an Integrated Component of System Development

Contacts: Beryl Hosack

301-921-3440

Bhosack@csc.com

Joe Guirreri

703-279-3588

Jguirrer@csc.com

Agenda

- Introduction
- Background
  - September 11 - Urgency
  - Directives and laws
  - Audits and Inspections
- Fundamental Issues in Protecting the NAS Infrastructure
- Base-lining the Security Architecture Up-Front
- Information Risk Management Model
  - How to do it, how to deliver it
- Summary/conclusion
- Questions?

CSC is Integrally involved in Security

- **NSC Infosec Assessment Training and Rating Program: evaluating NSA information security**
  - **Internationally recognized as one of 5 labs in United States authorized by NIST/NSA under NIAP to perform product & system security evaluations (common criteria ISO 15408)**
  - **helps agencies comply with Presidential Directive 63 (vulnerability assessments)**

- **DoD Computer Investigations Training Program**
  - **develop & deliver state-of-art computer investigation training courses for military law enforcement professionals including search & seizure, computer intrusions, forensic computer media analysis.**

CSC Recognized for Computer Security Expertise

- CSC Security Center of Excellence independently appraised at System Security Engineering Capability Maturity Model (SSE-CMM) Level 3 for INFOSEC assessments (Security Assessment Methodology)
- FAA:
  - Key player in FAA CIRC operations
  - Performing FAA Certifications and Accreditations
  - Key player in CPDLC (Data Link) Security Architecture formulation
  - CPDLC 1A Security Working Group
- Providing courseware across NASA through SOLAR system

Introduction/Background

- **Post September 11, security components are coming under intense scrutiny**
  - security becomes higher priority for the Federal sector
  - high priority for public as well
  - **Expectations of reduced operational costs & increased customer satisfaction place network security in the limelight to help achieve these strategic initiatives**
- NAS modernization efforts increasingly pressured to trade-off security, performance & cost across the NAS
- Reduction of NAS vulnerability dependent on:
  - integrated security approach supported by robust infrastructure
  - adoption of security best practices
  - continued development of a NAS-wide security architecture (within FAA guidelines & FAA internal ISSA)

Federal & FAA Directives Direct Our Actions

- **Continued emphasis on directive and law ensures high degree of integration within modernization efforts such as the NAS**
  - **OMB Circular 130,Computer Security Act of 1987,Clinger-Cohen,GISRAQ, FAA Directives**
  - **Standardized approach to security across the Federal Government, ensures security plans & processes support organizational missions & ensures actions are taken to certify systems & mitigate risk**
  - **Reduces implementation costs of security technologies**
  - **Assures adequate monitoring of attacks throughout Enterprise systems e.g. the NAS**

Developing an Architecture for security up-front provides enormous cost savings during implementation & maintenance. Security must not be "bolted-on after the fact.

Fundamental Issues in Protecting the NAS Infrastructure

Audit and liability driven

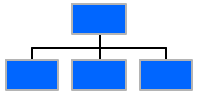
- Get infrastructure security under control
  - Secure distributed operation and administration with centralized coordination or control
  - Flexible, manageable, visible (COTS) security

Competition driven

- Reduce cost of maintaining infrastructure security
  - Shared infrastructure standardization for security services (e.g., identification, authorization, encryption, access control, digital signatures)
  - More reliable risk metrics that include operational consequences
- Expand and improve business by using new (secure) infrastructure services
  - Secure *COTs* applications

Base Line the Security Architecture Up Front

- Security architectures must be developed & integrated from the start of the development process



- Cohesively integrated infrastructures & architectures, beginning at the enterprise level are the key to NAS protection
- An array of technologies are being adopted to protect the NAS:
  - anti-virus tools, hardware based firewall technologies, security management strategies, intrusion detection, PKI, client-server certificates

- Other technology areas need more analysis:
  - Use of DMZs, implementing PKI,refinement of anti-virus tools, intrusion prevention and routers
- Increasingly strategic, complex or expensive security solutions are under consideration for adoption

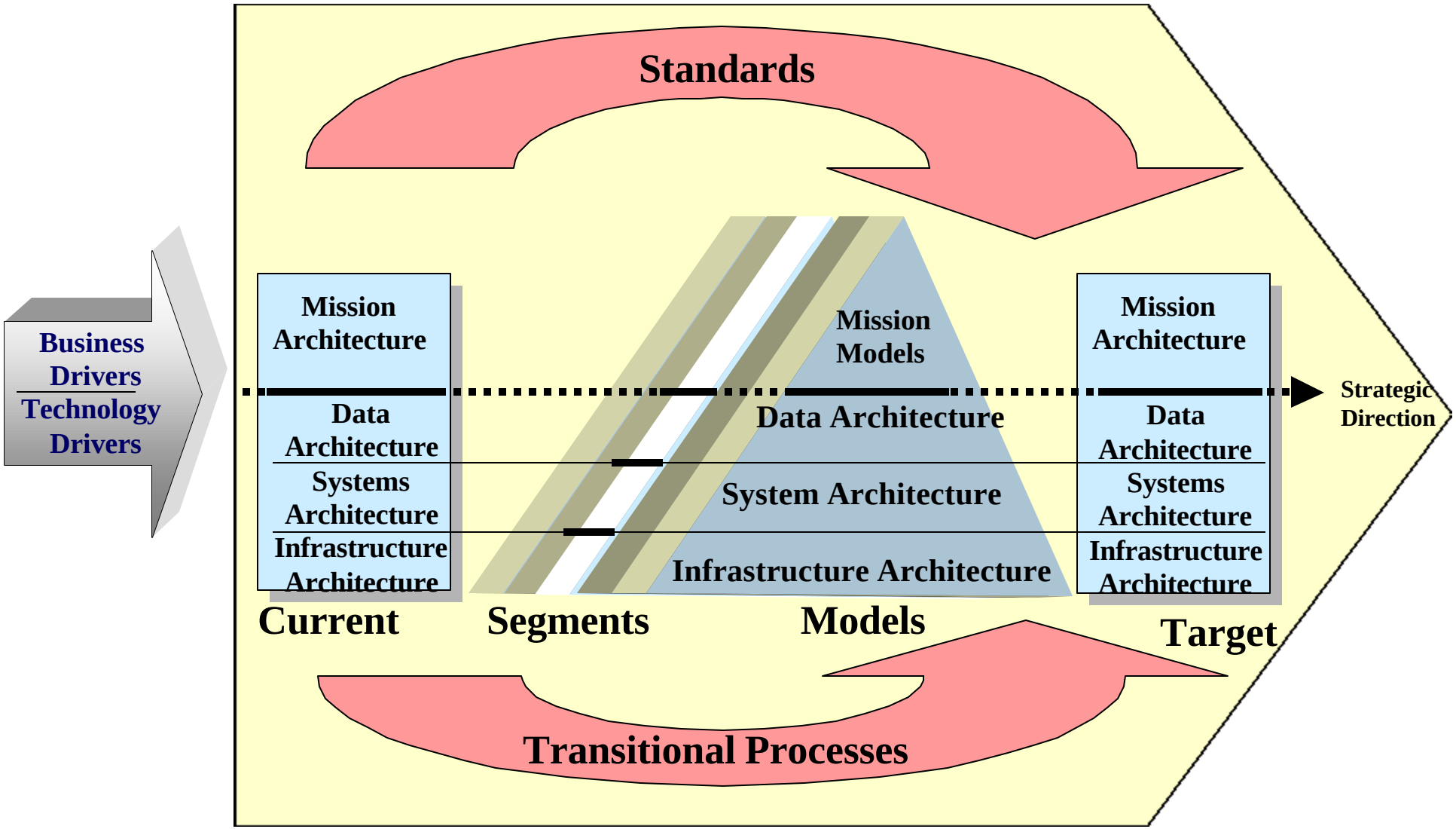
  - e.g. recently announced FAA directive to use PKI for ATN communications
  - e.g. new firewall models expected to improve performance and scale-ability while expanding protocol proxies & adding more to the devices including support for the new US/Gov approved AES (advanced Encryption Standard)

Up front base-lining reduces cost of insertion of new technologies as system matures

Designing Security Into the Architecture“Up-Front”

- **Enabling centralized Security Management:**
  - **tighter management integration of security solutions firewalls, VPNs, intrusion detection**
  - **Federal security organizations, reporting at a “high level”centralize security policies & standards**
- **Maturing Network Security service technologies e.g.PKI**
  - **more easily promoted for inclusion within the security architecture**
- **Consistent manner of embedding security standards within the infrastructure**

Architecture Framework



Embed Architecture into Total Security Capabilities

Analysis

- Security program and policy planning
  - Organization
  - Roles, responsibilities, authorities
  - Collaboration and coordination
- Security requirements analysis
  - Regulatory compliance
  - Audit compliance
  - Business value estimation
- Security compliance standards generation
- Security assessments
  - Strategic
  - Technical vulnerability
- Security architecture design
- Trust technology evaluations
- Security R&D and representation
- Security tool development, licensing, and support

Integration

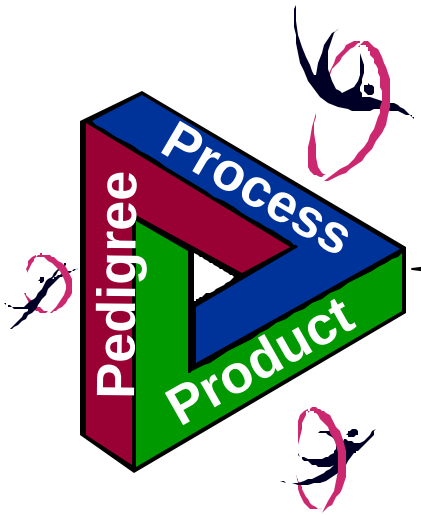
- Security test and evaluation of pilot implementations
- Security certification and accreditation/authorization (C&A)
- Security transformation and migration planning and execution
- Security technology introduction
  - Public Key Infrastructure (PKI)
  - Wireless
  - e-commerce assurance
- Information assurance technique training
- Application security requirements implementation and validation

Operation

- Client facility and asset protection
- Account security administration
- Security policy management
  - Control point devices (e.g., firewalls, switches, routers, VPNs)
  - Platform security
  - Directory services
- Security protection program
  - Vulnerability assessments & tracking
  - Vulnerability alert management
  - Anti-virus planning and execution
  - Audit readiness reinforcement
- Security compliance monitoring
  - Intrusion detection
  - Internet abuse prevention
  - Content filtering
  - Control point device policy compliance
  - Host (platform) configuration compliance
- Incident response and remediation
  - Computer forensics
- System security improvement program

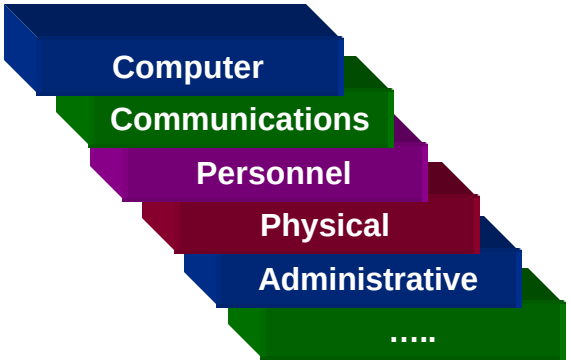
How To Do It
Information Risk Management Model

Combines all critical implementation success factors



A closed-loop, continuous process

Including all categories of safeguards



Covering all security services

How To Deliver It

From IRM Model to IRM *Program* (IRMP)

Model → **Program**

- Scope
- Security Standards
- Mission needs
- Current practices
- Legal requirements
- Acceptable risk threshold
- Data and process sensitivity
- Legacy obligations
- Evaluated security technology
- Operating model
- Cost constraints
- Schedule constraints

A Information Risk Management Approach (IRMA)
- IRMP Organization
- SWG operation
- BIAA
- 100-Day Plan
- Transition Security Handbook

B Security Compliance Standards (SCS)
- Equipment configuration standards
- Process action standards
- Staff capability standards

D Security Architecture Specification (SAS)

F Staff Security Services (SSS)
- Security Handbooks and Checklists
- Security Awareness Training
- Staff background checks

G Mission Continuity/Disaster Recovery Interface (MC/DRI)

H Special Security Needs (SSN)

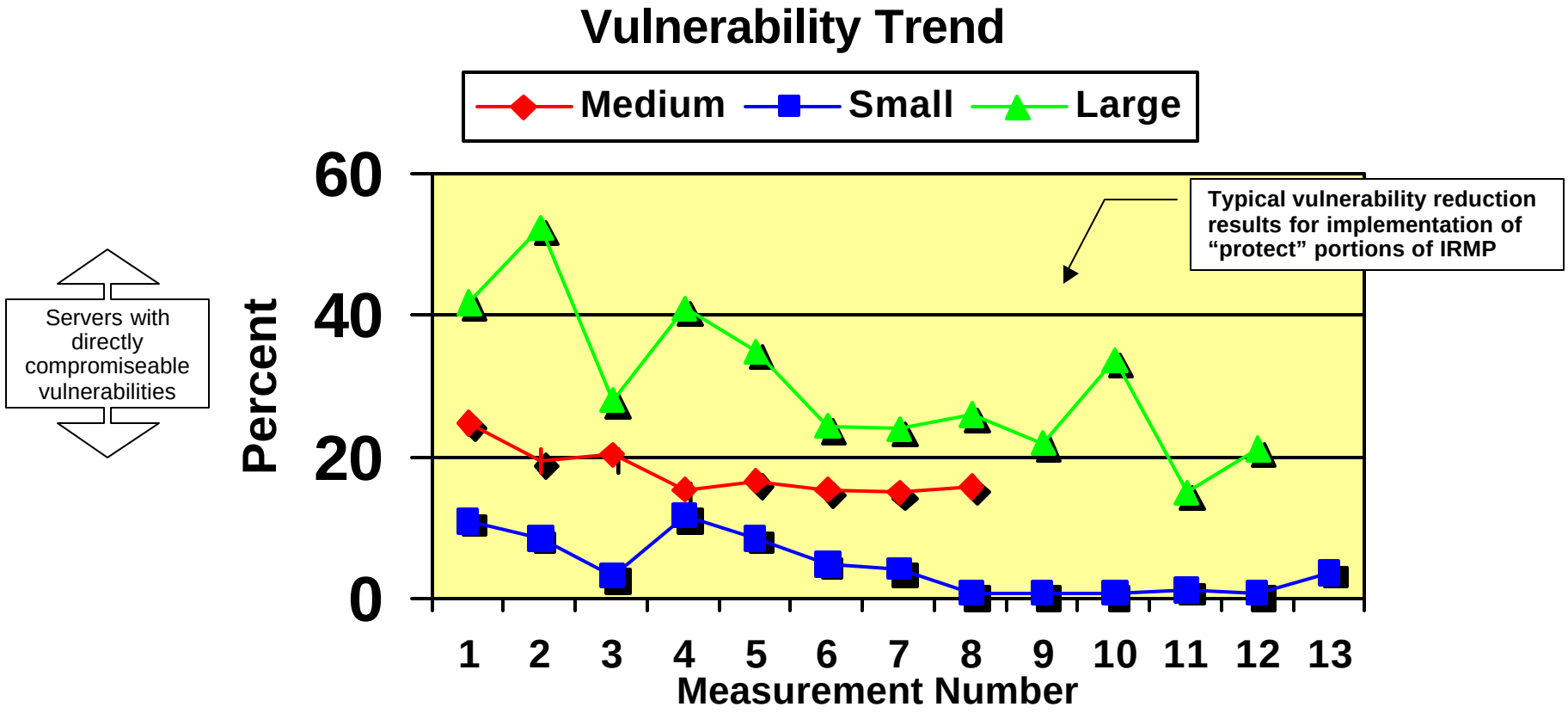
C Security Protection Program (SPP)
- Vulnerability Alert Management Process (VAMP)
- Vulnerability Assessment Program Plan (VAPP)
- Security Compliance and Monitoring Service (SCMS)
- Anti-virus Program Plan (AVPP)
- Incident Response Team (IRT)

E System Security Improvement Program (SSIP)

Legend

Typically targeted for accelerated implementation

Sample of Implementation Effectiveness
IRMP Results for Data Center Infrastructure Defense



Ensuring the Front-end Security Architecture Remains an Integrated Component of System Development

- **Provide Information Assurance Technique Training e.g.**
  - Information Security Concepts and Assessments,
  - Vulnerability Assessment and Mitigation
  - Security Technology and Administration
  - Security Incident Preparation and Response
  - Computer Forensics and Investigations
- **Architect for services including intrusion detection, compliance monitoring, incident response and recovery**
- Maintain Security Research Labs e.g.
  - Compliance Monitoring tools & techniques
  - Vulnerability assessment & remediation research
  - C&A process automation
  - Trust technology evaluations
  - Computer forensics
  - PKI integration and enablement
  - Secure e-Government in the back office
  - Threat analysis
  - Incident management
  - C&A automation

Summary

- Within the Federal Sector centralization of Security management & policy increasingly plays a significant role in infusing information security
  - process
  - awareness
  - technology
- To properly secure resources,security must be “built-in”
  - after-the-fact security is unworkable
- Security requirements & architectures must be developed from start of mission system architectural design process
- Applying this philosophy to NAS components will significantly reduce NAS vulnerability & achieve goal of protecting the NAS